We claim:

1. A method of authenticating communication between a first and a second party, the method comprising:

provisioning a first secure credential between the first party and the second party;

establishing a secure tunnel between the first party and the second party using the first secure credential;

authenticating a relationship between the first party and the second party within the secure tunnel using a second secure credential to establish an authorization policy; and

distributing an update to one of the first secure credential and the second secure credential within the secure tunnel to update the authorization policy.

2. The method set forth in claim 1 further comprising the step of protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user.

3. The method set forth in claim 1 wherein the step of provisioning occurs within a wired implementation.

4. The method set forth in claim 1 wherein the step of provisioning occurs within a wireless implementation.

5. The method set forth in claim 1 wherein the first secure credential is a protected access credential (PAC).

6. The method set forth in claim 5 wherein the protected access credential includes a protected access credential key.

7. The method set forth in claim 6 wherein the protected access credential key is a strong entropy key.

8. The method set forth in claim 7 wherein the entropy key is a 32-octet key.

9. The method set forth in claim 6 wherein the protected access credential includes a protected access credential opaque element.

10. The method set forth in claim 6 wherein the protected access credential includes a protected access credential information element.

11. The method set forth in claim 1 wherein the step of provisioning occurs through out-of-band mechanisms.

12. The method set forth in claim 1 wherein the step of provisioning occurs

through in-band mechanisms.

13. The method set forth in claim 1 wherein the step of establishing the secure tunnel includes the step of establishing a tunnel key using a symmetric cryptographic technique.

14. The method set forth in claim 13 wherein the step of establishing a tunnel key further includes the step of establishing a session_key_seed to be used in protecting the secure tunnel integrity and establishing a master session key.

15. The method set forth in claim 1 wherein the step of authenticating is performed using EAP-GTC.

16. The method set forth in claim 1 wherein the step of authenticating is performed using Microsoft MS-CHAP v2.

17. A system for communicating via a network, the system comprising:

means for providing a communication link between a first party and a second party;

means for provisioning a first secure credential between the first and the second party;

means for establishing a secure tunnel utilizing the first secure credential;

means for authenticating a relationship between the first party and the second party within the secure tunnel using a second secure credential to establish an authorization policy; and

means for delivering an update to one of the first secure credential and the second secure credential to update the authorization policy.

18. The system for communicating set forth in claim 17 wherein the communication link is a wireless network.

19. The system for communicating set forth in claim 17 wherein the communication link is a wired network.

20. The system for communicating set forth in claim 17 wherein the first secure credential is a protected access credential (PAC).

21. The system for communicating set forth in claim 18 wherein the wireless network is an 802.11 wireless network.

22. An article of manufacture embodied in a computer-readable medium for use in a processing system for communicating via a network, the article comprising:

a provisioning logic for causing the processing system to establish a shared secret between a first and a second party;

a tunnel establishment logic for causing the processing system to establish a secure tunnel based upon the shared secret;

an authentication logic for causing the processing system to authenticate a communication link between the first and the second party within the secure tunnel based upon a secure credential; and

a second provisioning logic for causing the processing system to provision an access; and

a delivery logic for causing the processing system to deliver an update to one of the shared secret and the secure credential via the network.

23. The article set forth in claim 22 wherein the tunnel establishment logic further includes a key generation logic for causing the processing system to generate a secure key for encrypting and signing a communication between the first party and the second party.